UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/721,713	11/27/2000	Jae-han Park	Q61823	4060

7590	07/16/2004

SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037-3202

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2131	6

DATE MAILED: 07/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 June 2004*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>27 November 2000</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date <u>5</u>.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Priority

1.   Applicant's claim for domestic priority under 35 U.S.C. 119(e) is acknowledged.

2.   The effective filing date for the subject matter defined in the pending claims in

this application is 11/25/1999 on the benefit of domestic provisional priority date.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 1 – 6, 8 – 10 and 13 are rejected under 35 U.S.C. under 35 U.S.C. 103(a)

as being unpatentable over Bluetooth (Specification of the Bluetooth System Version

1.0 A, July 26th 1999), hereinafter referred to as Bluetooth.

4.   As per claim 1, Bluetooth teaches an authentication method for establishing a

connection between devices that can wirelessly communicate data, the method

comprising the steps of:

a.   sending a first authentication-request message to another device to perform an

authentication procedure with the other device to which a connection is wanted

(Bluetooth: see for example, PART B, Section 3.2 Authentication page 194 and Section 3.3 Pairing page 196);

b.   sending a predetermined message according to a current operation mode to the other device and storing the predetermined message when an authentication-response message to the first authentication-request message is received (Bluetooth: see for example, PART C, Section 3.3.4 Creation of the Link Key, page 197);

5.   Bluetooth does not expressly teach:

c.   after performing the step (b), checking whether a received first message is a response message corresponding to the predetermined message when the first message from the other device is received;

6.   However, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the Bluetooth specification in an explicit way to accommodate, for the originator (or the verifier), checking whether a received first message is a response message corresponding to the predetermined message when the first message from the other device is received because (a) Bluetooth teaches mutual authentication is achieved by performing first the authentication procedure in one direction and, if successful, immediately followed by performing the authentication procedure in the reversed direction (Bluetooth: see for example, PART B, Section 14.2.2.2 Authentication 2nd Paragraph, page 154), and (b) Bluetooth further teaches the application should indicate who has to be authenticated by whom. Certain applications only require a one-way authentication. However, in some peer-to-peer communications, one might prefer a mutual authentication in which each unit is subsequently the

challenger (verifier) in two authentication procedures and thus the mutual authentication

is indeed an option during the authentication procedure (Bluetooth: see for example,

Figure 14.11 and PART B, Section 14.4 Authentication 4th Paragraph, page 170).

d.   sending a response message corresponding to a second authentication-request

message to the other device when the result of checking in the step (c) indicates that

the first message is the second authentication request message (Bluetooth: see for

example, Figure 14.11 and PART B, Section 14.4 Authentication 4th Paragraph, page

170, Line 7 – 9);

e.   after performing the step (d), checking whether a second message is a response

message corresponding to the predetermined message when the second message from

the other device is received (Bluetooth: see for example, PART C, Section 3.3.4

Creation of the Link Key, Line 6 – 8); and

f.   finishing the authentication procedure when the result of checking in the step (e)

indicates that the second message is a response message corresponding to the

predetermined message (Bluetooth: see for example, PART C, Section 3.3.4 Creation

of the Link Key, Line 9 – 16).

6.   As per claim 2 and 6, Bluetooth teaches the claimed invention as described

above (see claim 1 and 4 respectively). Bluetooth as modified further teaches in the

step (b), when the current operation mode is a pairing process, a message for

generating a link key is sent as the predetermined message and stored (Bluetooth: see

for example, PART C, Section 3.3.4 Creation of the Link Key, Line 6 – 16), and when

the current operation mode is not a pairing process, a message of

connection-establishment-completion is sent as the predetermined message and stored

(Bluetooth: see for example, PART C, Section 4 Connection Establishment,3rd

Paragraph); and the step (f) further comprises the sub-steps of:

(f1)   generating a link key before finishing the authentication procedure when the

current operation mode is a pairing process (Bluetooth: see for example, PART C,

Section 3.3.4 Creation of the Link Key, Line 6 – 16); and

(f2)   finishing the authentication procedure and establishing a connection to the other

device when the current operation mode is not a pairing process (Bluetooth: see for

example, PART C, Section 4 Connection Establishment,3rd Paragraph and Figure 4.1).

7.   As per claim 3, Bluetooth teaches the claimed invention as described above (see

claim 1). Bluetooth as modified further teaches the step (b) further comprises the

sub-steps of:

(b1)   checking whether the authentication-response message is valid using key

information and random information (Bluetooth: see for example, PART C, Section 3.2

Authentication and Section 3.2.1); and

(b2)   processing an authentication failure when the result of checking in the step (bl)

indicates that the authentication-response message is not valid (Bluetooth: see for

example, PART C, Section 3.2.1).

8.   As per claim 4, Bluetooth teaches the claimed invention as described above (see

claim 3). Bluetooth as modified further teaches in the step (b l), the key information is

held by the present device and the random information was used in sending the first

authentication message (Bluetooth: see for example, PART C, Section 3.2

Authentication).

9.   As per claim 5, Bluetooth teaches the claimed invention as described above (see

claim 1). Bluetooth as modified further teaches (g) finishing the authentication

procedure when the result of checking in the step (c) indicates that the received first

message is a response message corresponding to the predetermined message

(Bluetooth: see for example, PART C, Section 4 Connection Establishment, 3rd

Paragraph and Figure 4.1).

10.   As per claim 8, Bluetooth teaches the claimed invention as described above (see

claim 6). Bluetooth as modified further teaches in the step (d), when the predetermined

message received in the step (b) is a message for generating a link key, the present

device sends a response message corresponding to the message for generating a link

key to the other device, generates a link key, and then finishes the authentication

procedure (Bluetooth: see for example, PART C, Section 3.3.4 Creation of the Link Key,

Line 6 – 16 and Sequence 7); and when the predetermined message received in the

step (b) is a message of connection-establishment-completion, the present device

sends a response message corresponding to the message of connection-establishment

completion to the other device, finishes the authentication procedure, and then

establishes a connection to the other device (Bluetooth: see for example, PART C,

Section 4 Connection Establishment, 3rd Paragraph and Figure 4.1).

11.   As per claim 9, Bluetooth teaches the claimed invention as described above (see

claim 6). Bluetooth as modified further teaches the step (d) further comprises the

sub-steps of:

(d1)   checking whether the response message corresponding to the second

authentication-request message is valid when the response message corresponding to

the second authentication-request message is received by using random information

and key information (Bluetooth: see for example, Figure 14.11 and PART B, Section

14.4 Authentication 4th Paragraph, page 170); and

(d2)   processing an authentication failure when the result of checking in the step (dl)

indicates that the response message is not valid (Bluetooth: see for example, PART C,

Section 4 Connection Establishment, 3rd Paragraph and Figure 4.1).

12.   As per claim 10, Bluetooth teaches the claimed invention as described above

(see claim 9). Bluetooth as modified further teaches in the step (dl), the present device

holds the key information and the random information was used in sending the first

authentication message (Bluetooth: see for example, PART C, Section 3.2

Authentication).

13.   As per claim 13, Bluetooth teaches the claimed invention as described above

(see claim 10). Bluetooth as modified further teaches performing the authentication

procedure, when the authentication condition of the device that receives the

authentication request is set to require the mutual authentication procedure, the mutual

authentication procedure is performed by sending an authentication request message to

the device that requests an authentication (Bluetooth: see for example, Figure 14.11

and PART B, Section 14.4 Authentication 4th Paragraph, page 170).

14.   Claims 7, 11, 12 and 14 are rejected under 35 U.S.C. under 35 U.S.C. 103(a) as

being unpatentable over Bluetooth (Specification of the Bluetooth System Version 1.0 A,

July 26th 1999), hereinafter referred to as Bluetooth, in view of Shona (Patent Number:

5799085), hereinafter referred to as Shona.

15.   As per claim 7, Bluetooth teaches an authentication method for establishing a

connection between devices that can wirelessly communicate data, the method

comprising the steps of:

a.   sending a response message corresponding to a first authentication request

message when the first authentication-request message from another device that wants

to establish a connection is received (Bluetooth: see for example, PART C, Section 3.2

Authentication and Section 3.3.1);

b.   Bluetooth does not expressly teach, after performing the step (a), checking an

authentication condition of the present device when a predetermined message from the

other device is received.

16.   Shona teaches after performing the step (a), checking an authentication

condition of the present device when a predetermined message from the other device is

received (Shona: see for example, Column 5 Line 61 – 67).

17.   It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Shona within the system of Bluetooth as

modified because (a) Bluetooth teaches mutual authentication is achieved by

performing first the authentication procedure in one direction and, if successful,

immediately followed by performing the authentication procedure in the reversed

direction (Bluetooth: see for example, PART B, Section 14.2.2.2 Authentication 2nd

Paragraph, page 154), and (b) Bluetooth further teaches the application should indicate

who has to be authenticated by whom. Certain applications only require a one-way

authentication. However, in some peer-to-peer communications, one might prefer a

mutual authentication in which each unit is subsequently the challenger (verifier) in two

authentication procedures and thus the mutual authentication is indeed an option during

the authentication procedure (Bluetooth: see for example, Figure 14.11 and PART B,

Section 14.4 Authentication 4th Paragraph, page 170), and (c) Shona teaches a method

of effecting mutual authentication between two entities that the authentication condition

is determined by the setting of a mutual authentication enabling flag (Shona: see for

example, Column 5 Line 61 – 67).

19.   Bluetooth as modified further teaches:

c.   storing the predetermined message and sending a second authentication-request

message to the other device when the result of checking indicates that a mutual

authentication is required (Bluetooth: see for example, PART B, Section 14.2.2.2

Authentication 2nd Paragraph, page 154 & Figure 14.11 and PART B, Section 14.4

Authentication 4th Paragraph, page 170).

d.   after performing the step (c), sending a response message corresponding to the

message stored in the step (c) to the other device when a response message from the

other device corresponding to the second authentication-request message is received,

and finishing the authentication procedure (Bluetooth: see for example, PART C,

Section 4 Connection Establishment,3rd Paragraph and Figure 4.1).

19.   As per claim 12, Bluetooth teaches determining whether an authentication

procedure for establishing a connection between devices that want to communicate

data is performed as a unilateral authentication procedure or as a mutual authentication

procedure (Bluetooth: see for example, PART B, Section 14.2.2.2 Authentication 2nd

Paragraph, page 154 & Figure 14.11 and PART B, Section 14.4 Authentication 4th

Paragraph, page 170). However, Bluetooth does not expressly teach this decision is

determined according to an authentication condition which enables receiving an

authentication request in the two devices that can communicate data; and performing

the authentication procedure.

20.   Shona teaches the decision is based on an authentication condition which

enables receiving an authentication request in the two devices that can communicate

data; and performing the authentication procedure (Shona: see for example, Column 5

Line 61 – 67).

21.   It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Shona within the system of Bluetooth as

modified because (a) Bluetooth teaches mutual authentication is achieved by

performing first the authentication procedure in one direction and, if successful,

immediately followed by performing the authentication procedure in the reversed

direction (Bluetooth: see for example, PART B, Section 14.2.2.2 Authentication 2nd

Paragraph, page 154), and (b) Bluetooth further teaches the application should indicate

who has to be authenticated by whom. Certain applications only require a one-way

authentication. However, in some peer-to-peer communications, one might prefer a

mutual authentication in which each unit is subsequently the challenger (verifier) in two

authentication procedures and thus the mutual authentication is indeed an option during

the authentication procedure (Bluetooth: see for example, Figure 14.11 and PART B,

Section 14.4 Authentication 4th Paragraph, page 170), and (c) Shona teaches a method

of effecting mutual authentication between two entities that the authentication condition

is determined by the setting of an mutual authentication enabling flag (Shona: see for

example, Column 5 Line 61 – 67).

22.   As per claim 11 and 14, Bluetooth teaches the claimed invention as described

above (see claim 6 and 10 respectively). Bluetooth as modified does not expressly

teach in the step (b) authentication enable information is checked as the authentication

condition.

23.   Shona further teaches in the step (b) authentication enable information is

checked as the authentication condition (Shona: see for example, Column 5 Line 61 –

67: An mutual authentication flag is set to enable the mutual authentication function

between two entities).

24.   Same rationale of combination applies herein as above in rejecting Claim 12.
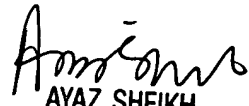
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100